Deloitte.

A treatment plan for a ransomware attack

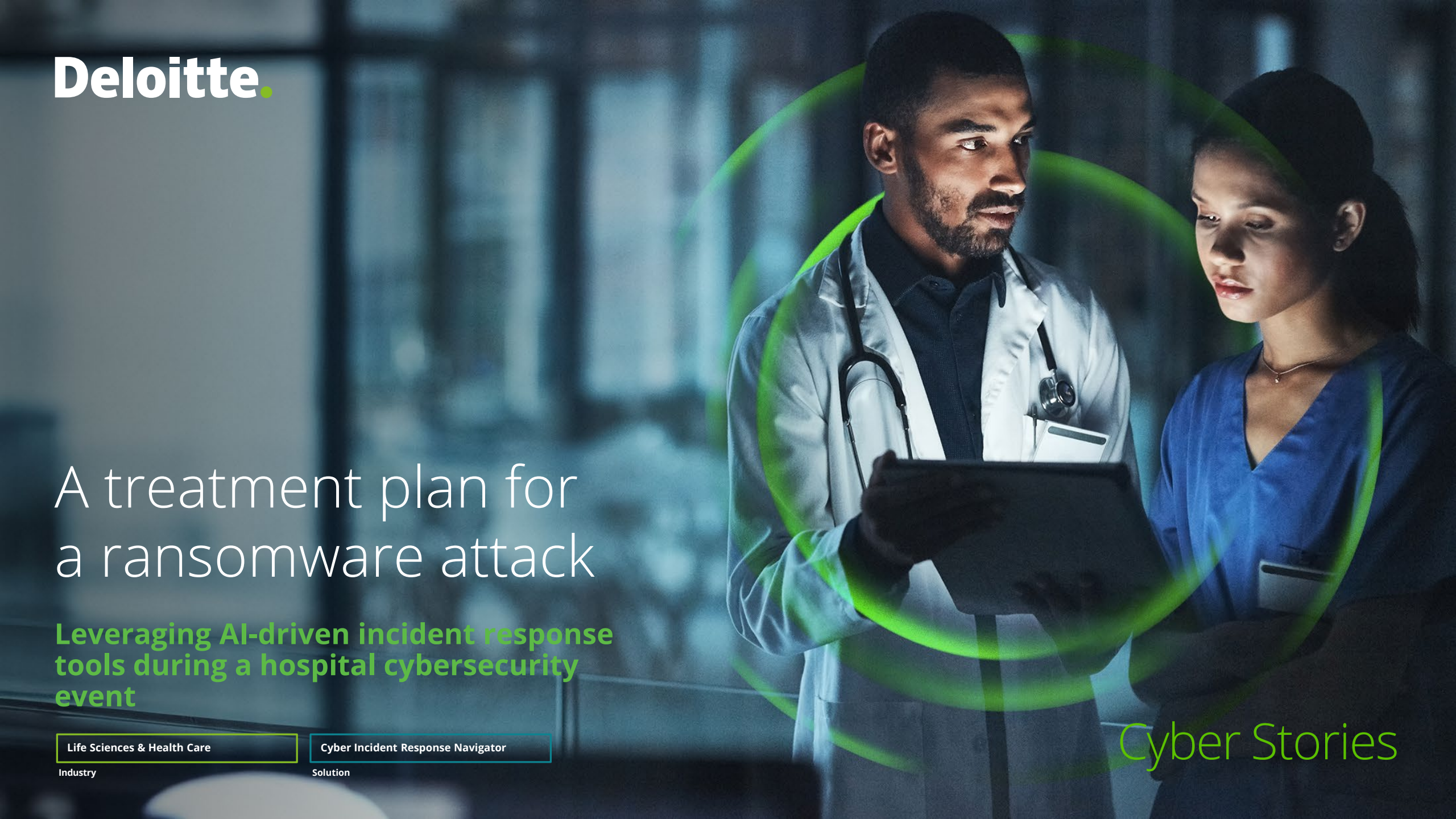
Leveraging AI-driven incident response tools during a hospital cybersecurity event

Life Sciences & Health Care

Industry

Cyber Incident Response Navigator

Solution



Cyber Stories

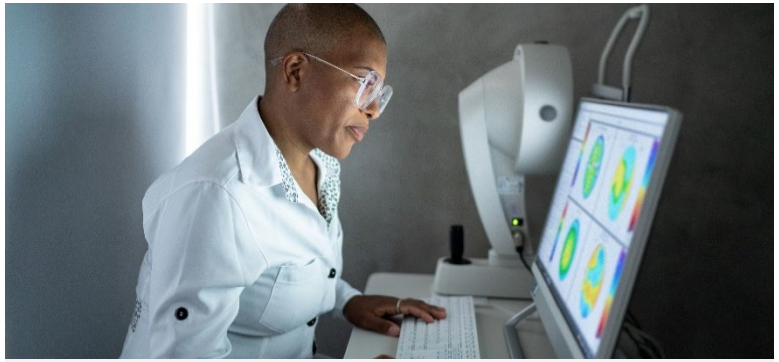
The starting point

Digital data is the lifeblood of hospitals and health systems today. Patient records, diagnostic results, scheduling information, billing records, care instructions, and more—it all resides in networked systems that provide medical professionals, patients, caregivers, and other authorized stakeholders with the information they need to ensure appropriate care, coordinate logistics, and make informed decisions.

That cache of data and networks is a prime target for cyber threat actors who are looking to exploit systems, disrupt operations, or steal sensitive information. For one large regional hospital in North America, the cyber risks became very real, very quickly.

Early one morning, the hospital's cyber incident monitoring platform began providing alerts. Unusual network activity indicated that an incident was unfolding—with the telltale signs of a ransomware attack. The clock was ticking. The hospital's information technology (IT) and cybersecurity team knew that they had hours, maybe minutes, until a widescale ransomware "detonation" would leave systems and data inaccessible. Unaddressed, the attack could put patients' lives and health at risk, and force staff to rely on manual processes such as hand-written notes for recording and sharing critical information.

Rapid action was key to defusing the ransomware attack, but the hospital wanted to ensure that any actions would be decisive, thorough, and guided by industry-leading practices for addressing cyber threats. Hospital leaders asked for clear visibility for stakeholders throughout the response.



Factors in focus

- Rapidly unfolding ransomware attack
- Organization's high dependence on digital data and systems for delivering patient care
- Need to respond with speed and confidence, aligned with leading practices for the industry and the threat

The way forward

The hospital had already been working with Deloitte so when the ransomware attack began unfolding, they quickly called in the Deloitte team for critical guidance and IR services.

Collaborating with the hospital's team, Deloitte leveraged its Cyber Incident Response Navigator (CIRN) to guide incident response. Enabling Deloitte teams to respond to cyber incidents rapidly and confidently, the AI-powered solution acts as a semi-autonomous platform to provide real-time, tailored insights for cyber incident management. It draws from a vast repository of incident and threat intelligence sources—from Deloitte's global network, as well as third-party, public, and proprietary threat data—to streamline and accelerate incident management, automate workflows, and provide visibility for stakeholders.

Deloitte used the IR Navigator to provide benchmarking and analytics for planning each phase of the incident response, from investigation to recovery, to help align timelines and activities. Through AI-driven response playbooks, the platform also outlined specific steps for teams to take in each phase—including reminders for specific remediation steps, as well as alerts for engaging with stakeholders such as legal, insurance, or regulatory authorities at key points in incident response.

Insights to inspire

Leverage intelligent technology to guide and streamline the steps of incident response—so IR teams can focus on solving more challenging problems.

When responding to an incident, draw on cybersecurity teams based in other global regions to help provide uninterrupted, round-the-clock support.

Leveraging the IR Navigator, Deloitte was able to quickly isolate and investigate the threat, focusing more on deeper problem-solving. The work included seeking out forgotten-about firewalls and other potential threat entry points, identifying any tools the threat actor might have dropped into the hospital's systems, determining the impact on patient data, and doing the hands-on work of cleaning and rebuilding systems.

As part of the response, Deloitte enlisted a wide range of professionals, including specialists in cybersecurity/endpoint software, firewall specialists, and industry specialists. Deloitte also relied on its incident responders based in Australia, helping ensure that IR and remediation activities were carried out around the clock, for a faster recovery and return to normal operations.

The achievements

Working in close coordination with the Deloitte team, the hospital was able to isolate the ransomware threat in a matter of days and thoroughly investigate the potential impact—returning to baseline business operations within one week. At the two-week mark, the recovery was considered complete, and the hospital was once again operating normally. Meanwhile, key data and insights generated during the response were fed back into Deloitte's Cyber Incident Response Navigator—to help improve the platform's knowledge base and performance for future engagements.

Ultimately, by working with Deloitte and leveraging the IR Navigator, the hospital was able to realize several benefits, including:

Responsiveness

Streamlined, accelerated incident response to support a faster recovery

Detection

Increased confidence in addressing the threat, anchored in leading practices and relevant threat/industry playbooks

Protection

Enhanced ability to protect the organization's operations and mission, to safeguard human health and save lives

Resilience

Greater resilience for the organization's business and critical systems overall

Readiness

Improved cybersecurity posture for addressing new threats in the future

Let’s talk cyber

How prepared is your organization for a ransomware attack? And how will you neutralize the next incident that threatens to disrupt your business? Discover how Deloitte’s worldwide team of industry-focused cybersecurity specialists can help you respond with speed and confidence. Contact us to get the conversation started.

deloitte.com/cyber

Contacts

John Gelinne
Global Cyber Resilience Leader
Deloitte US
jgelinne@deloitte.com

Marco Manglaviti
IR Navigator
Deloitte Canada
mmanglaviti@deloitte.ca

Bryson Tan
IR Leader
Deloitte Canada
brtan@deloitte.ca

Deloitte.

Cyber Stories